PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ^{7} : **H04N 7/10**	**A1**	**(11) International Publication Number:** **WO 00/59217** **(43) International Publication Date:** 5 October 2000 (05.10.00)

(21) International Application Number: PCT/US00/08618

(22) International Filing Date: 30 March 2000 (30.03.00)

(30) Priority Data:

60/127,127	31 March 1999 (31.03.99)	US
09/458,619	10 December 1999 (10.12.99)	US

(71) Applicant: DIVA SYSTEMS CORPORATION [US/US]; 800 Saginaw Drive, Redwood City, CA 94063 (US).

(72) Inventor: BERTRAM, Michael, C.; 417–17 Camille Circle, San Jose, CA 95134 (US).

(74) Agents: MOSER, Raymond, R. et al.; Thomason Moser and Patterson, LLP, 2–40 Bridge Avenue, P.O. Box 8160, Red Bank, NJ 07701 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

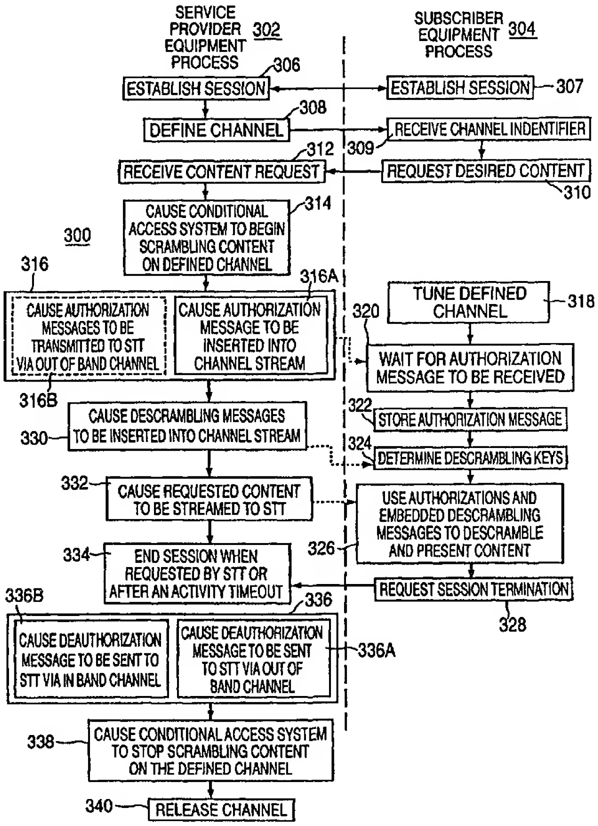
Published

With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHOD AND APPARATUS FOR PERFORMING SESSION BASED CONDITIONAL ACCESS

(57) Abstract

A method and apparatus for enabling session–based conditional access to on–demand content of variable duration by scrambling (314) a program stream provided to a set top terminal via a defined communications channel; communicating (316) to the set top terminal while establishing a session, via one of the defined communications channel and an out–of–band communications channel, an authorization message and descrambling message suitable for determining a descrambling key for descrambling the program stream; and including (330), within the program stream being scrambled, content requested by the set top terminal.


SERVICE PROVIDER EQUIPMENT PROCESS
302
SUBSCRIBER EQUIPMENT PROCESS
304
306
ESTABLISH SESSION
ESTABLISH SESSION
307
308
DEFINE CHANNEL
RECEIVE CHANNEL INDENTIFIER
312
309
RECEIVE CONTENT REQUEST
REQUEST DESIRED CONTENT
310
CAUSE CONDITIONAL ACCESS SYSTEM TO BEGIN SCRAMBLING CONTENT ON DEFINED CHANNEL
314
300
316
316A
CAUSE AUTHORIZATION MESSAGES TO BE TRANSMITTED TO STT VIA OUT OF BAND CHANNEL
CAUSE AUTHORIZATION MESSAGE TO BE INSERTED INTO CHANNEL STREAM
TUNE DEFINED CHANNEL
318
320
WAIT FOR AUTHORIZATION MESSAGE TO BE RECEIVED
316B
CAUSE DESCRAMBLING MESSAGES TO BE INSERTED INTO CHANNEL STREAM
330
322
STORE AUTHORIZATION MESSAGE
324
DETERMINE DESCRAMBLING KEYS
332
CAUSE REQUESTED CONTENT TO BE STREAMED TO STT
USE AUTHORIZATIONS AND EMBEDDED DESCRAMBLING MESSAGES TO DESCRAMBLE AND PRESENT CONTENT
326
334
END SESSION WHEN REQUESTED BY STT OR AFTER AN ACTIVITY TIMEOUT
REQUEST SESSION TERMINATION
328
336B
336
CAUSE DEAUTHORIZATION MESSAGE TO BE SENT TO STT VIA IN BAND CHANNEL
CAUSE DEAUTHORIZATION MESSAGE TO BE SENT TO STT VIA OUT OF BAND CHANNEL
336A
338
CAUSE CONDITIONAL ACCESS SYSTEM TO STOP SCRAMBLING CONTENT ON THE DEFINED CHANNEL
340
RELEASE CHANNEL

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

METHOD AND APPARATUS FOR PERFORMING SESSION BASED CONDITIONAL ACCESS

CROSS REFERENCE TO RELATED APPLICATIONS

This application claims benefit of U.S. Provisional Patent Application Serial Number 60/127,127 (attorney docket number 037), which was filed on March 31, 1999 and is incorporated herein by reference in its entirety.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to an information distribution system such as a video-on-demand (VOD) system. More particularly, the present invention relates to a method and apparatus for providing session-based conditional access to on-demand content of variable duration within a conditional access information distribution system.

2. Description of the Background Art

In an information distribution system, such as video on demand (VOD) system, an information provider (e.g., a head-end in a cable television system) must control of the distribution of requested information to ensure that only an appropriate information consumer (e.g., a requesting VOD subscriber) is able to utilize the distributed information. To provide this functionality, information distribution systems are often implemented using a conditional access system.

VOD systems providing content encoded according to the various Moving Pictures Experts Group (MPEG) standards are known. For example, a first standard known as MPEG-1 refers to ISO/IEC standards 11172, which is incorporated herein by reference in its entirety. A second standard known as MPEG-2 refers to ISO/IEC standards 13818, which is incorporated herein by reference in its entirety. Additionally, a compressed digital video system is described in the Advanced Television Systems

Committee (ATSC) digital television standard document A/53, incorporated herein by reference.

MPEG-based conditional access systems typically have three main attributes: the scrambling (or encoding) of MPEG streams, the transmission of de-scrambling messages and the transmission of authorization messages. De-scrambling messages are embedded in the MPEG transport stream and used by information consumer equipment (e.g., set top terminals) to descramble the content. Authorization messages can be sent with the scrambled stream or by some other route and are used to authorize set top terminals to use the descrambling information.

Conditional access systems are typically adapted to a broadcast service model, whereby scrambling is performed on a "per service" basis or a "per event" basis. Per service scrambling supports protection of subscription channels where access is provided on a 24 hour basis over an extended period of time. Per event scrambling supports pay per view services where access is provided for a short, pre-scheduled period of time.

Unfortunately, the broadcast service model does not adequately support the unique needs of video on demand (i.e., non-broadcast) services. Specifically, per service scrambling provides limited protection in on demand situations where multiple users have exclusive access to the same channel separated by time. Per event scrambling does not accommodate the need for protection for unscheduled access periods of variable duration.

Therefore, it is seen to be desirable to provide a method and apparatus enabling session-based conditional access to on-demand content of variable duration.

SUMMARY OF THE INVENTION

The disadvantages heretofore associated with the prior art are overcome by the present invention of a method and apparatus for enabling session-based conditional access to on-demand content of variable.

Specifically, in a conditional access information distribution system, a method according to the invention comprises the steps of: scrambling a program stream provided to a set top terminal via a defined communications channel; communicating to the set top terminal, via one of the defined communications channel and an out-of-band communications channel, an authorization message and descrambling message suitable for determining a descrambling key for descrambling the program stream; and including, within the program stream being scrambled, content requested by the set top terminal.

BRIEF DESCRIPTION OF THE DRAWINGS

The teachings of the present invention can be readily understood by considering the following detailed description in conjunction with the accompanying drawings, in which:

FIG. 1 depicts a high level block diagram of an interactive information distribution system;

FIG. 2 depicts a block diagram of the set top terminal suitable for use in the interactive information distribution system of FIG. 1; and

FIG. 3 depicts a flow diagram of an illustrative implementation of an session-based conditional access method as performed on both service provider equipment and subscriber equipment within the interactive information distribution system of FIG. 1.

To facilitate understanding, identical reference numerals have been used, where possible, to designate identical elements that are common to the figures.

DETAILED DESCRIPTION

Throughout this description various terms are used to describe the invention. Unless modified by the following description, several of the terms are defined as follows: Scrambling comprises a method of protecting a data stream by transforming the value of bits in the stream based on a given key. For the purposes of this disclosure scrambling has the same meaning as encrypting. Descrambling comprises a method for transforming data stream bits back to their original value based on the use of a key. For the purposes of this description disclosure has the same meaning as decryption. A conditional access (CA) system is a system that generates keys, descrambling messages, and authorization messages supporting the scrambling and descrambling of, e.g., MPEG encoded programs. A descrambling message comprises a conditional access message containing descrambling information for a particular MPEG program. The descrambling information may contain the descrambling key or the information a Set Top Box (or boxes) needs to generate the descrambling key. An authorization message comprises a conditional access message authorizing a particular Set Top Box to use a descrambling key to descramble a particular MPEG program.

FIG. 1 depicts a high level block diagram of an interactive information distribution system. Specifically, FIG. 1 depicts a high level block diagram of an interactive information distribution system 100 containing the present invention. The system 100 contains service provider equipment 102, a communications network 104 and subscriber equipment 106_n, where n is an integer greater than zero.

The service provider equipment 102 comprises a content and asset storage module 125, a session controller 145, a transport processor 150 and a conditional access system 160. Briefly, the session controller 145, in response to a request from subscriber equipment 106, causes requested content and associated assets to be retrieved from the content and asset storage module 125 and provided to the transport processor 150. The transport processor 150 combines or multiplexes the content and asset data to provide an output data stream for the requesting subscriber. The output data stream is conditioned for transport to the requested subscriber via a forward application transport channel (FATC) within the distribution network 104. The conditional access system 160, in response to a service scrambling request (SSR) signal produced by the session controller 145, generates scrambling keys SK, descrambling messages DM and authorization messages AM. The scrambling keys are utilized by the transport processor 150 to scramble the content and/or assets provided to the requesting subscriber via the output data stream. The descrambling messages DM and authorization messages AM are provided to the requesting subscriber via the forward application transport channel. The authorization may also be provided to the subscriber via the forward data channel (FDC). The requesting subscriber equipment receives and decodes the requested content and/or assets using, as necessary, the descrambling messages DM and authorization messages AM provided via the FATC and/or FDC.

The content and asset storage module 125 is used to store content such as movies, television programs and other information offerings of the interactive information distribution system 100 of FIG. 1. Additionally, the content and asset storage module 125 is used to store assets such as bit map imagery, graphic overlay, control scripts and the like. The assets may comprise, for example, navigation assets that are used by a set top terminal to interactively navigate, and select for viewing, the offerings or content available from the service provider equipment 102. The content and asset storage module 125, in response to a control SC produced by the session controller 145, provides content and/or asset data to the transport processor 150.

The session controller 145 (or session manager) provides session control of the information flowing to and from the content and asset storage module 125, and may be generally described as a system providing or controlling communications between, for example, a cable system head-end and one or more set top terminals. The session controller 145 produces the storage control signal SC for controlling and communicating with the content and asset storage module 125, and a transport processor control signal TPC for controlling and communicating with the transport processor 150. In response to a user request for particular content, the session controller 145 causes the requested content file and any associated assets to be streamed from the content and asset storage module 125 to the transport processor 150.

The conditional access system 160, in response to a service scrambling request (SSR) signal produced by the session controller 145, generates scrambling keys SK, descrambling messages DM and authorization messages AM. Based on the service scrambling request, the scrambling keys SK and descrambling messages DM are provided to the transport processor 150. Additionally, the authorization messages AM are provided to the transport processor 150 if the FATC is used to provide authorization messages to the set top terminals. Optionally, the authorization messages AM are provided to the session controller 145 for subsequent coupling to the appropriate set top terminal via the forward data channel FDC.

The session controller 145 sends data, such as commands, to set top terminals via a forward data channel (FDC). The session controller 145 receives data, such as information stream requests and session initiation data (set top identification, capability and the like) via a reverse data channel (RDC). The FDC and RDC are supported by the distribution network 104 and comprise relatively low bandwidth data channels, such as one-two megabits per second data channels utilizing QPSK, QAM, or other modulation techniques. The FDC and RDC are also known as "out-of-band" channels, while the relatively high bandwidth forward application transport channel (FATC) is also known as an "in-band" channel. The session controller 145 contains an interface device for sending control information via the forward data channel FDC and receiving control information and request information via the reverse data channel RDC using the so-called "out-of-band" carrier frequencies.

The transport processor 150 accomplishes all of the forward content channel transmission interface requirements of the system 100 of FIG. 1. Specifically, the transport processor 150 is coupled to subscriber equipment via the forward applications transport channel (FATC). The FATC is supported by the distribution network 104 and comprises a relatively high bandwidth communications channel well suited to carrying video, audio and data such as, for example, multiplexed MPEG-2 transport packets. It should be noted that data normally conveyed to a set top terminal via the FDC may be included in the FATC data stream.

The transport processor 150 is capable of scrambling content and of inserting descrambling messages and authorization messages into a transport stream being provided to an output channel. The transport processor 150 utilizes descrambling keys SK provided by the conditional access system 160 to scramble specific content, or content on a specific channel. The transport processor 150 embeds the descrambling messages DM and authorization messages AM provided by the conditional access system 160 within the scrambled content or channel (that is, in-band communications to a requesting STT). Optionally, the authorization messages AM are provided to the appropriate STT via the forward data channel FDC (that is, via the out-of-band communication to the STT). The transport processor 150 contains a digital video modulator for modulating the content and/or asset streams provided by the content and asset storage module 125 on to one or more carrier frequencies that are compatible with the transmission requirements of the network 104. That is, the transport processor 150 is capable of providing a plurality of scrambled or unscrambled content and/or asset streams modulated onto various carrier frequencies suitable for use in the distribution network 104. It should be noted that in the exemplary embodiment the descrambling messages DM are never sent by the forward data channel FDC, since the descrambling messages and the content to be descrambled using the descrambling messages are related to each other by a fairly close timing relationship, such that the set top terminal receiving descrambling messages DM out of sync with content to be descrambled will likely be unable to perform the descrambling operation.

The transport processor 150 also contains a modulator for modulating the combined content and asset stream onto one or more carrier frequencies for transmission on the FATC, the so-called “in-band” carrier frequencies.

The session controller 145 scrambles the retrieved content provided by the content and asset storage module 125 and inserts descrambling messages and authorization messages into a transport stream including the scrambled content. That is, the session controller 145 scrambles the content on the channel intended to be used by a set top terminal requesting the scrambled content. In addition, the session controller 145 inserts descrambling messages and authorization messages into the transport stream provided by that channel to the requesting set top terminal such that the set top terminal may access the scrambled content in the manner previously described.

In a scrambling mode of operation, the session controller 145 provides a service scrambler request (SSR) signal to the conditional access system 160 including the channel number or identifier of the channel to be scrambled (this channel identifier is also provided to the STT requesting the scrambled content stream). The service scrambler request SSR signal also includes information indicative of the service of the content to be scrambled, precisely which content is to be scrambled, and which channel is to transport the scrambled content to the requesting STT.

The distribution network 104 can be any one of a number of conventional broadband communications networks that are available such as a fiber optic network, a telephone network, existing cable television network and the like. For example, if the network is a hybrid fiber-coax network, the transmission transport technique used in both forward channels may be modeled after the Moving Pictures Expert Group (MPEG) transport protocol for the transmission of video data streams. In general, the transport mechanism for both of the forward channels that transport information to the set top terminal must be able to carry unidirectional, asynchronous packetized data such as that defined in the MPEG video and audio signal transmission protocol, and the like. There are a number of such transport protocols available.

The subscriber equipment 106 comprises a set top terminal or a set top box 136, a display device 140 (e.g. a conventional television) and a user input device 138 (e.g. a remote control device). Each set top terminal 136 receives the data streams from the FATC, demodulates the received data streams and, in the case of video streams, processes the demodulated video streams for subsequent display on the display device 140. In the case of receiving scrambled data streams, the STT descrambles the received data streams using the descrambling messages DM provided to the STT via the FATC. The STT uses the authorization messages AM provided via the FATC or FDC to determine if a descrambling of the received scrambled stream is authorized. In addition, the set top terminal 136 accepts commands from the remote control input device 138 or other input device. These commands are formatted, modulated, and transmitted through the distribution network 104 to the session controller 145. Typically, this transmission is accomplished through the reverse data channel RDC. These commands are preferably transmitted through the same network used to transmit information to the set top terminal. However, the RDC coupling the set top terminal to the provider equipment 102 may be a separate network, e.g. a FATC through a television cable network and an RDC through a telephone network. The telephone network could also support the FDC.

FIG. 2 depicts a high level block diagram of a set top terminal (STT) suitable for use in the interactive information distribution system of FIG. 1. A set top terminal (or set top box) comprises a device capable of receiving and decompressing content within, e.g., an MPEG transport stream to produce a resulting signal(s) suitable for use by a presentation device such as a display device. Set top terminals are also capable of conditional access message processing and transport stream descrambling.

Specifically, FIG. 2 depicts a block diagram of an exemplary embodiment of the set top terminal 136 interactive information distribution system of FIG. 1. The STT 136 of FIG. 2 comprises a transceiver 200, a central processing unit (CPU) 212 and a display driver 222. The CPU 212 is supported by random access memory (RAM) 220, read only memory (ROM) 218 and various support circuits 216 such as clocks, power supply, an infrared receiver and the like. The transceiver 200 contains a diplexer 202, a back channel transmitter 208, an information channel receiver 204, a conditional access module 205, a command channel receiver 210 and an transport demultiplexer and decoder 206. The diplexer 202 couples the three channels carried by a single cable within the network to the transmitter and receivers.

Each receiver 204 and 210 contains a tuner, amplifiers, filters, a demodulator, and a depacketizer. As such, the receivers tune, downconvert, and depacketize the signals from the cable network in a conventional manner. The information channel receiver 204 contains a conventional QAM demodulator such as a model BCM3115 manufactured by the Broadcom Corporation. Other such demodulators are well-known in the communications arts and could be used in this application. However, this particular QAM demodulator also contains a built in "out-of-band" QPSK demodulator for handling command channel data carried by the forward command channel. As such, a single integrated circuit demodulates both subscriber requested information (audio and video) as well as command data.

The transport demultiplexer and decoder 206 processes the data packets carrying subscriber requested information produced by the QAM demodulator into useable signals for the end user display, e.g., television, home studio, video recorder and the like. The decoder is coupled to a dynamic random access memory (DRAM) to facilitate decoding of the data packets and processing of applets, as shall be discussed below. The signals for display are conventionally processed by a display driver 222 to produce a video signal suitable for use by, e.g., the display device 140.

The transport demultiplexer and decoder 206 also extracts authorization and descrambling messages from the received data stream and provides the extracted authorization and descrambling messages to the conditional access module 205.

The conditional access module 205, illustratively a smart card or dedicated chip set, accepts authorization and descrambling messages extracted by the transport demultiplexer and decoder 206 and responsively provides descrambling keys for the selected content stream when appropriately authorized.

The transport demultiplexer and decoder 206 utilizes the descrambling keys provided by the conditional access module 205 to descramble or decrypt the selected content stream prior to decoding the stream to form appropriate presentation signals.

The demodulated QPSK signal provides command and control information to the CPU 212 for generating a graphical user interface upon the display device 140. The CPU 212, operating in combination with the decoder 206 as well as a video signal from the information channel, produces screen displayed buttons, icons and graphical regions with which a subscriber interacts using, for example, a remote control device. User interaction comprises, for example, the navigation of a graphical user interface to select one of a plurality of available program titles for immediate or future presentation.

Session control commands are implemented by the session controller 145 and not the set top terminal 136 alone. Each command is implemented by the execution of an applet by the set top terminal 136. The applet is transmitted to the STT by the session manager in response to, e.g., back channel requests transmitted by the STT. The applets control both information sessions, e.g., the presentation of video to the television screen, and navigator functions, e.g., the menus that facilitate selection of a video program. As such, particular commands include, but are not limited to, information or menu navigation commands, movie start at beginning, movie start at the middle, play, stop, rewind, forward, pause, and the like. These presentation and navigation control commands are sent via a back channel transmitter 208 using binary phase shift key (BPSK) modulation.

FIG. 3 depicts a flow diagram of an illustrative implementation of an session-based conditional access method as performed on both service provider equipment and subscriber equipment within the interactive information distribution system of FIG. 1. Specifically, FIG. 3 is divided into two columns, namely: a service provider equipment process column 302 and a subscriber equipment process column 304.

The method 300 of FIG. 3 begins at steps 306 and 307 where, respectively, the service provider equipment 102 and subscriber equipment 106establish a session with each other.

At step 308, the service provider equipment 102 identifies or defines a channel identifier (e.g., a physical and logical transmission channel) and communicates the defined channel identifier to the subscriber equipment. The subscriber equipment receives the defined channel identifier at step 309.

At step 310, the subscriber equipment requests desired content from the service provider equipment. At step 312 the service provider equipment receives the content request from the subscriber equipment.

At step 314, the provider equipment causes the conditional access system to begin scrambling content on the defined channel. That is, the session controller 145 issues a service scrambling request (SSR) to the conditional access system 160. The conditional access system 160, in response to the SSR, generates scrambling keys SK, descrambling messages DM and authorization messages AM which are provided to the session controller 145 and to the transport processor 160. The transport processor 160 utilizes the scrambling keys SK provided by the conditional access system 160 to scramble specific content on the defined channel or all content on the defined channel.

At step 316, the provider equipment 102 causes the authorization messages to be inserted into the FATC stream (i.e., the in-band channel) 316A or transmitted to the STT via FDC (i.e., the out-of-band channel) 316B. That is, transport processor 150 embeds the authorization messages AM provided by the conditional access system 160 within the scrambled content provided via the forward applications transport channel FATC (i.e., in-band communication to the STT) 116A. Optionally, the authorization messages AM are provided to the appropriate STT via the forward data channel FDC (i.e., out-of-band communication to the STT).

At step 330, the provider equipment causes the descrambling messages DM to be inserted into the FATC stream (i.e., the in-band channel).

At step 332, the provider equipment begins streaming the requested content to the STT via the defined channel. That is, the requested content is streamed to the requesting STT via the defined channel. Since information provided by the defined channel is now being scrambled by the transport processor 150, the requested content is scrambled prior to being coupled to the STT. Additionally, the descrambling messages and, optionally, authorization messages are embedded in the scrambled stream provided to the STT.

At step 318, the subscriber equipment tunes the defined channel, illustratively, a QAM channel comprising a transport streams including video and audio streams associated with the requested content. It should be noted that the requested content is not yet available to the subscriber at this time. Specifically, the requested content has not yet been streamed to the subscriber via the defined channel (see step 332) and the subscriber has not received (per step 320) or used (per step 328) the authorization and descrambling messages necessary to decrypt and present the requested (scrambled) content.

At step 320, the subscriber equipment waits for an authorization message to be received. That is, a requesting set top terminal 136, having tuned to the channel indicated during session setup, monitors the incoming data on the in-band channel (FATC) or the out-of-band channel (FDC) until an authorization message provided by the conditional access system 160 is received.

At step 322, upon receiving the authorization message associated with the defined channel (per step 320), the authorization message is stored within the subscriber equipment conditional access module 205. The received authorization message for the requested content will be subsequently used by the set top terminal to derive the descrambling key from the descrambling messages embedded in the defined channel used to provide the requested content to the subscriber.

At step 324, the stored authorization is used to determine the descrambling keys. That is, if the conditional access module 205 has received the appropriate authorization messages for the channel containing the requested content, the conditional access module will derive the necessary keys from the embedded descrambling messages.

At step 326, the descrambling keys are used to descramble the requested content. That is, the subscriber equipment utilizes the descrambling keys derived from the descrambling messages to descramble the content and present the descrambled content on, e.g., a display device. This occurs when the subscriber equipment begins receiving the scrambled requested content (step 332).

At step 328, upon concluding the presentation of the desired content, the subscriber equipment requests that the session be terminated.

At step 334, the service provider equipment stops streaming the requested content when either a session termination request is received or when the STT has been inactive for a predetermined period of time.

At step 336, the service provider equipment causes a de-authorization message to be sent to the STT via the FDC (i.e., the out-of-band channel) 336A or via the FATC (i.e., the in-band channel) 336B. That is, transport processor 150 embeds the de-authorization messages DM provided by the conditional access system 160 within the scrambled content provided via the forward applications transport channel FATC or within the forward data channel FDC. By including the de-authorization messages DM in either the in-band (step 336B) or out-of-band (step 336A) channels, the descrambling keys derived from the previous authorization messages will be inactivated. The method 300 then proceeds to step 338.

At step 338, the provider equipment causes the conditional access system to stop scrambling content on the defined channel. The method 300 then proceeds to step 340, where the service provider equipment releases the defined channel such that the channel may be utilized by another session between the service provider equipment and another subscriber.

It should be noted that while the steps comprising the above-described method 300 of FIG. 3 are depicted as being in a particular order, variations of that order are contemplated by the inventor and are within the scope of the invention. For example, the STT can request content at the establishment of a session or upon receiving the service or authorization from the provider equipment (step 320). In either case, it is desirable for the STT to receive the service or authorization from the provider equipment 102 prior to receiving scrambled content. In this manner the STT is able to descramble all of the requested content.

To ensure that the STT receives the service or authorization from the provider equipment prior to receiving scrambled content, the requested content may be transmitted without scrambling until the service or authorization is transmitted or transmission of the scrambled requested content may be delayed until the service or authorization is transmitted. The first case provides low-latency content delivery, while the second case provides complete protection of all content.

Additional requests for content are satisfied by the session controller 145 by transmitting the additional requested content within the same scrambled service being provided to the STT via the defined channel.

The above-described invention extends current conditional access capabilities to provide on-demand security for session-based content access. Advantageously, the invention avoids pre-scheduling and fixed duration restrictions associated with an service-based conditional access approach by adapting the a service- or channel-based conditional access capability. In this manner, inadequacies of shared service access are avoided while conditional access capabilities providing low latency on-demand authorization capabilities are enabled.

Although various embodiments which incorporate the teachings of the present invention have been shown and described in detail herein, those skilled in the art can readily devise many other varied embodiments that still incorporate these teachings.

What is claimed is:

1. In an information distribution system utilizing conditional access, a method comprising the steps of:

scrambling (314) a program stream provided to a set top terminal via a defined communications channel;

communicating (316) to said set top terminal while establishing a session, via one of said defined communications channel and an out-of-band communications channel, an authorization message and descrambling message suitable for determining a descrambling key for descrambling said program stream; and

including (330), within said program stream being scrambled, content requested by said set top terminal.

2. The method of claim 1, wherein said defined channel comprises a quadrature amplitude modulated (QAM) channel and said program stream comprises an MPEG transport stream.

3. The method of claim 1, further comprising the steps of:

communicating (336) to said set top terminal, via one of said defined communications channel and said out-of-band communications channel, a de-authorization message, said de-authorization message being communicated in response to a session terminating event.

4. The method of claim 3, wherein said session terminating event comprises one of a session termination request being received from said subscriber and a period of subscriber inactivity exceeding a predetermined time interval.

5. The method of claim 1, wherein said authorization message and descrambling message are communicated to said subscriber after said content is included in said scrambled program stream, said method further comprising the step of:

repeating, for a predetermined period of time, said step of communicating said authorization message and descrambling message to said subscriber

6. The method of claim 1, wherein said information distribution system comprises an information on demand system.

7. In conditional access information distribution system comprising provider equipment for providing information to subscribers via a communications channel, a method comprising the steps of:

scrambling (314) a program stream provided (332) to a set top terminal via a defined communications channel;

communicating (316) to said set top terminal, via one of said defined communications channel (316A) and an out-of-band communications channel (316B), an authorization message and descrambling message suitable for determining a descrambling key for descrambling said program stream; and

including (332), within said program stream being scrambled, content requested by said set top terminal.

8. The method of claim 7, wherein said defined channel comprises a quadrature amplitude modulated (QAM) channel and said program stream comprises an MPEG transports stream.

9. The method of claim 7, further comprising the steps of:

communicating (336) to said set top terminal, via one of said defined communications channel and said out-of-band communications channel, a de-authorization message, said de-authorization message being communicated in response to a session terminating event.

10. The method of claim 9, wherein said session terminating event comprises one of a session termination request being received from said subscriber and a period of subscriber inactivity exceeding a predetermined time interval.

11. The method of claim 7, wherein said authorization message and descrambling message are communicated to said subscriber after said content is included in said scrambled program stream, said method further comprising the step of:

repeating, for a predetermined period of time, said step of communicating said authorization message and descrambling message to said subscriber

12. The method of claim 7, wherein said conditional access information distribution system comprises an information on demand system.

13. In conditional access information distribution system (100) comprising provider equipment (102) for providing information to subscribers (106) via a communications channel, provider apparatus comprising:

a conditional access system (160), for scrambling a program stream to produce a scrambled program stream; and

a session manager (145), for providing said scrambled program stream to a set top terminal via a defined communications channel, said session manager including within said scrambled program stream content requested by said set top terminal;

said session manager communicating to said set top terminal, via one of said defined communications channel and an out-of-band communications channel, an authorization message and descrambling message suitable for determining a descrambling key for descrambling said program stream;

said conditional access system providing said authorization message and said descrambling message to said session manager.

14. The provider apparatus of claim 13, further comprising an information server (125), for providing said requested content to said session manager.

15. The provider apparatus of claim 13, wherein said defined channel comprises a quadrature amplitude modulated (QAM) channel and said program stream comprises an MPEG transports stream.

16. The provider apparatus of claim 13, wherein:

said session manager, in response to a session terminating event, communicates a de-authorization message to said set top terminal via one of said defined communications channel and said out-of-band communications channel.

17. The provider apparatus of claim 16, wherein said session terminating event comprises one of a session termination request being received from said subscriber and a period of subscriber inactivity exceeding a predetermined time interval.

18. The provider apparatus of claim 13, further comprising:

a data storage module, coupled to the information server, for storing content.

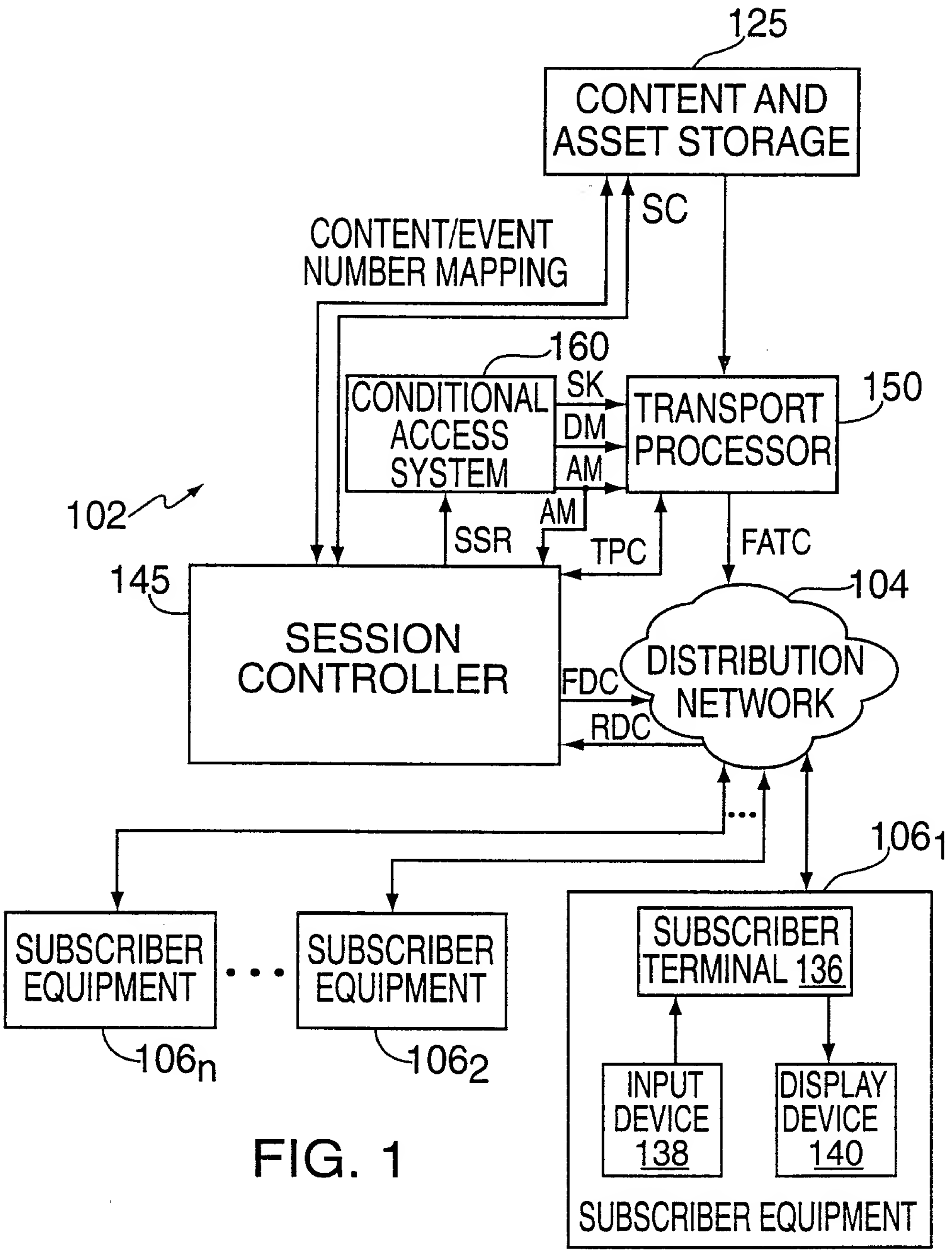

125
CONTENT AND ASSET STORAGE
CONTENT/EVENT NUMBER MAPPING
SC
160
CONDITIONAL ACCESS SYSTEM
SK
DM
AM
TRANSPORT PROCESSOR
150
102
AM
SSR
TPC
FATC
145
SESSION CONTROLLER
104
DISTRIBUTION NETWORK
FDC
RDC
106_1
SUBSCRIBER TERMINAL 136
INPUT DEVICE 138
DISPLAY DEVICE 140
SUBSCRIBER EQUIPMENT
SUBSCRIBER EQUIPMENT
SUBSCRIBER EQUIPMENT
106_n
106_2

FIG. 1

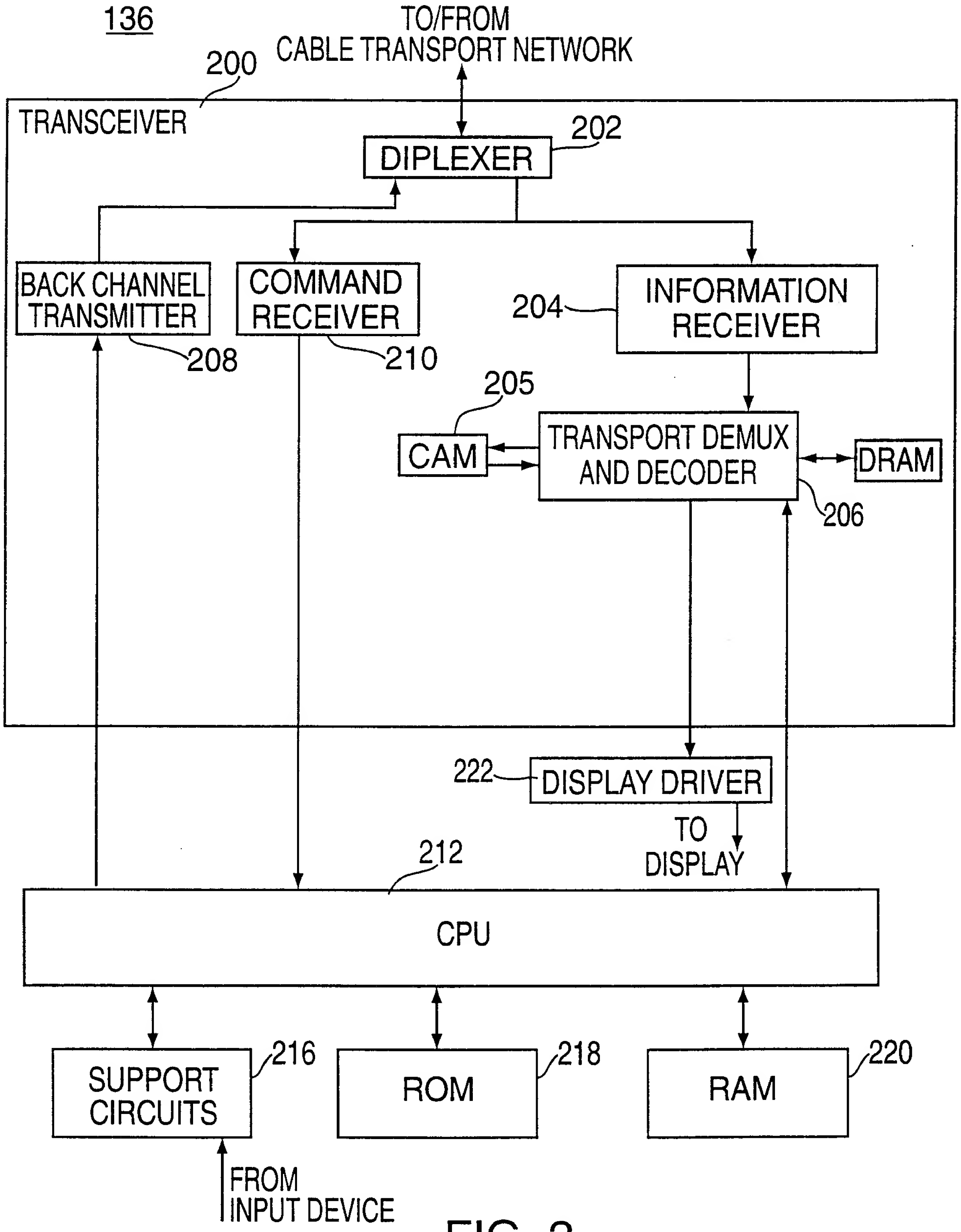

136
TO/FROM
CABLE TRANSPORT NETWORK
200
TRANSCEIVER
DIPLEXER
202
BACK CHANNEL
TRANSMITTER
208
COMMAND
RECEIVER
210
204
INFORMATION
RECEIVER
205
CAM
TRANSPORT DEMUX
AND DECODER
DRAM
206
222
DISPLAY DRIVER
TO
DISPLAY
212
CPU
SUPPORT
CIRCUITS
216
ROM
218
RAM
220
FROM
INPUT DEVICE

FIG. 2

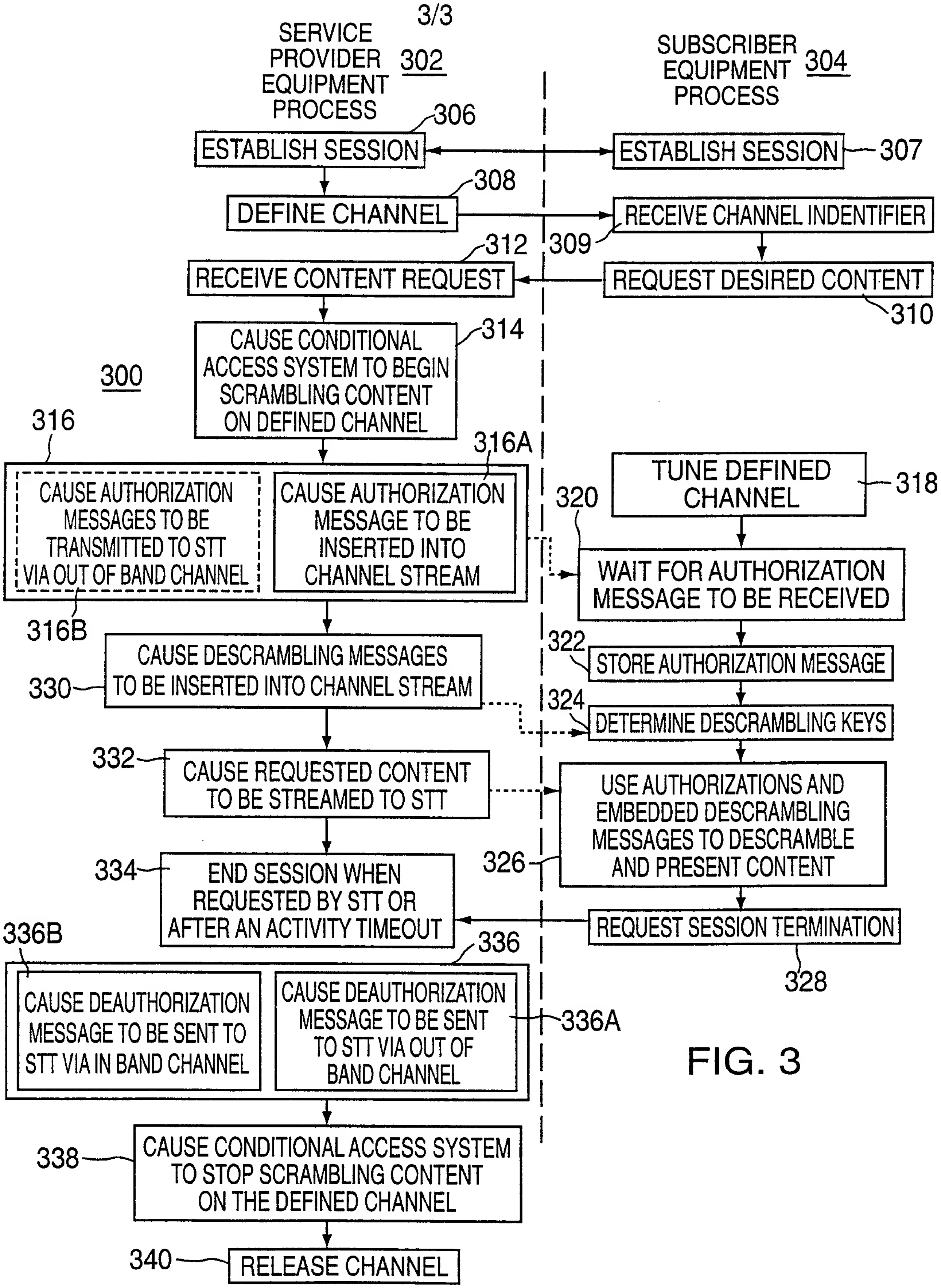

SERVICE PROVIDER EQUIPMENT PROCESS
302
SUBSCRIBER EQUIPMENT PROCESS
304
306
ESTABLISH SESSION
ESTABLISH SESSION
307
308
DEFINE CHANNEL
RECEIVE CHANNEL INDENTIFIER
309
312
RECEIVE CONTENT REQUEST
REQUEST DESIRED CONTENT
310
314
CAUSE CONDITIONAL ACCESS SYSTEM TO BEGIN SCRAMBLING CONTENT ON DEFINED CHANNEL
300
316
316A
CAUSE AUTHORIZATION MESSAGES TO BE TRANSMITTED TO STT VIA OUT OF BAND CHANNEL
CAUSE AUTHORIZATION MESSAGE TO BE INSERTED INTO CHANNEL STREAM
316B
TUNE DEFINED CHANNEL
318
320
WAIT FOR AUTHORIZATION MESSAGE TO BE RECEIVED
CAUSE DESCRAMBLING MESSAGES TO BE INSERTED INTO CHANNEL STREAM
330
322
STORE AUTHORIZATION MESSAGE
324
DETERMINE DESCRAMBLING KEYS
332
CAUSE REQUESTED CONTENT TO BE STREAMED TO STT
USE AUTHORIZATIONS AND EMBEDDED DESCRAMBLING MESSAGES TO DESCRAMBLE AND PRESENT CONTENT
326
334
END SESSION WHEN REQUESTED BY STT OR AFTER AN ACTIVITY TIMEOUT
REQUEST SESSION TERMINATION
328
336B
336
CAUSE DEAUTHORIZATION MESSAGE TO BE SENT TO STT VIA IN BAND CHANNEL
CAUSE DEAUTHORIZATION MESSAGE TO BE SENT TO STT VIA OUT OF BAND CHANNEL
336A
338
CAUSE CONDITIONAL ACCESS SYSTEM TO STOP SCRAMBLING CONTENT ON THE DEFINED CHANNEL
340
RELEASE CHANNEL

FIG. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/08618

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :H04N 7/10
US CL :709/217; 348/5.5, 12
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 709/217-219; 348/5.5, 6, 7, 10, 12, 13

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EAST

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y,E	US 6,055, 315 A (DOYLE ET AL.) 25 APRIL 2000, FIGURES 1-5.	1,7
Y	US 5,485, 221 A (BANKER ET AL.) 16 JANUARY 1996, FIGURES 1-3.	1,7

□ Further documents are listed in the continuation of Box C. □ See patent family annex.

*	Special categories of cited documents	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance		
"E"	earlier document published on or after the international filing date	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed	"&"	document member of the same patent family

Date of the actual completion of the international search 05 JULY 2000	Date of mailing of the international search report 18 AUG 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer NATHAN J. FLYNN Eugenia Logan Telephone No. (703) 308-0000